Don’t Let These Technology Missteps Be Your Client’s Downfall

By Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Lawyers know from personal experience how consuming technology can be. And they know how easy it is to overshare on social media, click on something they didn’t mean to, or say something foolish after having too many libations. Your clients are no different in their reliance on technology but they are going through one of the most emotional and stressful periods of their lives.

This is where the missteps come in. Clients’ technology, especially their usage of social media and text messaging, tend to become part of the divorce and discovery process. Throw into the mix a soon-to-be ex-spouse, a hotly-contested divorce, custody battles and maybe the involvement of third party lovers and you have the ingredients for an explosion that you will not want to sort out before a judge.

Happily, there is advice that you can give your clients at the onset of the engagement to help them protect themselves. Think of it as a “Do Not Do List.”

We live in an extremely over-shared world, where people often feel compelled to post videos and pictures of everything they do, believe in or feel at any given moment. Social media can be a goldmine of information for opposing attorneys. Too often clients post information that may be harmful to their case, such as the picture of their most recent blind-date to a local winery or their spur-of-the-moment extravagant trip to Bali for a little “R&R.” Surely your client will be asked about these should opposing counsel get hold of them, and instead of just being innocent posts that were shared, your client is now labeled an adulterer, a drunk and accused of hiding assets – after all, how could they afford that luxurious trip and with whom did they go?

The best technological advice you can give your client is to stop using their social media accounts entirely. It may be hard, but quitting cold-turkey may be the best thing they can do to help their case. Many social media providers such as Facebook and Instagram have options to disable, rather than to delete accounts, so that after the divorce is finalized or the ink has dried on the settlement papers, your client is free to post again, however unwise their posts. And so long as you disable or deactivate an account rather than deleting it, you will not face accusations of spoliation.

Switching gears for a moment, we want to discuss something that most clients lose during the divorce process - common-sense. Clients are often willing to go to immeasurable lengths to get information on their soon-to-be ex-spouse to help strengthen their negotiating position or to gain any perceived upper-hand in the process. This often includes breaking the law. Accessing a password-protected account of the other party, especially when there is an expectation of privacy, should be discouraged at all costs. There are legal routes to get the same information and they should always be the paths taken. Some examples of accounts that should never be accessed include the other party’s:

- New (non-marital) bank account, credit card account, loan records or stock trading account
- Personal or business email accounts

- Social media accounts, such as Facebook, Instagram, Snapchat
- Apple iCloud accounts (www.icloud.com)

It is always better to obtain information legally – and to keep your client out of hot water with the judge and the law. And no, the "accounts are shared" excuse is not a get-out-of-jail-free-card. Your client better have a good criminal defense attorney on speed-dial if they opt to ignore these warnings.

While on the topic of "doing things the right way," your client should never steal or "borrow" a personal device of the other party, to have it analyzed by a digital forensics company or private investigator. Again, there is a right way and wrong way to do this. As their attorney, you can request the devices and information contained on them through the discovery process, via a subpoena or court motion. Having your client steal the devices in the dead-of night to have them covertly inspected (or worse, installing spyware) is not the best course of action. More on spyware in just a bit. Having said that, there is no restriction for making a forensic copy for preservation purposes. You just can't go snooping around before getting court approval or agreement of the device owner.

While any respectable digital forensics company would immediately inform your client of the limitations of the work they can legally perform, your client is better off being educated beforehand. Generally, a marital device can be forensically (and legally) copied or preserved, and that may be all that can be done at that moment, without further authorization from the court to access "password-protected" materials. The marital device can be forensically imaged in the same way that either party could legally make a backup of the device or its data. But if one party has a password-protected email or any other sort of account on the marital computer, the laws protect the privacy of that data. Installing spyware, cracking or guessing passwords – all of that is not permitted.

Shopping around for someone to get you "all of the data" from a device, regardless of its legal protections, will only lead to more problems, including inadmissibility problems, and yes, possible criminal charges. While attorneys can explain any state-specific "gray areas" to their clients, the best advice is to respect the privacy of password-protected data unless there is an agreement with the other party to grant access or a court order authorizing access.

In the realm of divorce, spyware, hacking, interception of communications and electronically monitoring someone's actions, are often used and should always be avoided. Your client should never install software on a computer system or mobile device to monitor a former (or soon to be former) spouse's activity. They should never modify the settings of an email account to auto-forward messages. There is a list a mile long of things they should NOT do in an attempt to monitor their former partner. One of the more popular mechanisms these days is to use the "Find My iPhone" feature of a jointly used Apple iCloud account to track the other party's movements and location. This usually works when one party isn't aware of what an iCloud account even is or which one of their devices is set up to use it! Sharing iCloud accounts is a big no-no in our book. Not only can your spouse track your location within a few feet, but any messages, emails, photographs, videos and other application data may be accessible to them as well – especially if the iCloud account is being used on multiple devices. If your client uses an Apple iPhone, iPad or Mac computer system, we recommend that your clients disconnect any previously configured iCloud account and create a new one for their new life. They can accomplish that through the settings of their device or through the www.icloud.com website.

One of the more interesting scenarios that we have encountered involved a client who used a Google NEST security camera installed at a jointly owned-rental property, to monitor their soon-to-be ex-spouse. The former spouse was allegedly dating the renter. The monitoring led the client to catch their spouse committing adultery, which they thought would lead to a quick resolution and settlement of the divorce. Instead, there were more headaches for the client, including another civil suit and a pending criminal investigation, in addition to the divorce matter. Was it worth it? The client probably doesn't think that now. If you don't know the legality of your client's actions, it certainly wouldn't hurt to error on the side of caution, saving them future self-inflicted heartburn.

Not every divorce is desired by both parties. Sometimes, your client's hand is forced by the actions of the other party. One thing that your spurned client should not do, is take revenge – either physically or online. Sadly, we have seen a significant rise in revenge porn cases.

More and more spurned partners have turned to the idea of "getting back" at their former spouse by posting private photographs and videos, taken or received through the previous relationship, on the Internet. There are many websites dedicated to revenge porn, so that should not come as a surprise. As more victims have sought legal recourse for these actions, 40 states currently have laws banning revenge porn, while other states have harassment laws that may be applied to seek justice for the victims in these criminal matters.

Some people believe they can get away with this type of conduct without having the evidence traced back to them, but in reality, they are setting themselves up for criminal charges. The websites used to upload and post these types of photos maintain logs that can help to identify where the activity originated from and ultimately, who uploaded the photos or videos. Internet service providers, including mobile carriers, also maintain logs. These logs cannot simply be deleted by your client, so it would be best to advise them against any type of this activity from the onset of the engagement.

Another potentially criminal action that we often consult on is spoliation. The intentional deletion of potentially relevant data can derail your client's divorce case. It's far better for the data to be properly preserved, searched and produced, then to have to explain to a judge why your client was deleting emails or text messages, in violation of a discovery order, subpoena or document request. The problem for clients is that there are digital forensic companies that can recover deleted information, and produce it in court. There may even be evidence to recover that shows who deleted the information and exactly when it was deleted.

We've been involved with many matters where evidence has shown mass purging right before the date when a party was required to produce evidence in response to a subpoena or court order. We have also seen Internet searches for how to successfully delete text messages or emails. Boy, do the judges love to see those searches! They are equally incensed to hear how a phone mysteriously was stolen or lost, right before being requested for analysis. We've received countless phones that have been water damaged, factory reset or just plain lost, immediately prior to a court deadline to produce them. All we can say is that this practice is frowned upon and may lead to some serious legal consequences for your client. Oh, and don't think that replacing the phone with another model or an identical model can't be determined through analysis. No matter what, hiding, destroying or otherwise obstructing the discovery of evidence will not result in your client having a good outcome in court.

Protecting privacy and personal communications is important to most people. However, installing an application on your phone or computer that provisions secure encrypted communication may not be a good thing, especially if the intent was to securely communicate with a paramour. Signal, WhatsApp and Telegram are several apps used for secure communications. Even though you won't be able to obtain the content of the communications, you may be able to retrieve contacts and times/dates of the communications. Technically, there is nothing wrong with using these secure communications apps. However, if the paramour's ID is found on your spouse's phone and the paramour has also installed the same app with your spouse's ID, the inference may be all it takes to sway the court.

Now that we have spent some time at length going over what technology missteps your client should avoid – why should your client listen to our advice?

Roughly 25% of our digital forensics cases are family law matters. We've seen firsthand the trouble clients get into when they access accounts without authorization. We've seen lawsuits filed in response to the installation of spyware or using a security camera to remotely and surreptitiously monitor their former spouse. We've seen the weight of evidence lessoned due to the manner in which it was obtained. There have even been occasions where a party has been jailed due to the spoliation of evidence. It's rare, but we've seen it happen.

Judges have little or no tolerance for your client's foolish or illegal actions. They have zero tolerance for your client lying to the court. A little stern guidance at the outset of an engagement can benefit them greatly – if you can get them to listen, which is sometimes challenging. It is certainly worth the effort to try. You would hate to have a misstep affect the outcome of a custody or spousal support battle.

We have all become too reliant on technology in our day-to-day lives, for both work and personal usage. Even during some of the most stressful situations your clients will ever face as they go through the divorce process, they need to maintain (instead of lose) their common-sense when it comes to the usage of technology. The legal consequences of missteps are real – and often devastating.

The authors are the President, Vice President and CEO of Sensei Enterprises, Inc., a cybersecurity, information technology and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com